Magic-Numbers

James Philip Rowell

May 14, 2024 (v36.2)

In the film "School of Rock", Jack Black's character Mr. S. has to demonstrate one of his "teaching methods" for the school principal Miss Mullins. So he improvises "The Math Song", the final line being "… ♫ yes it's nine ♫… and that's a magic-number ♫… "

I believe Jack was tipping his hat to the "Schoolhouse Rock" song "3 Is A Magic Number" which most kids from the 70's/80's know.

However referring to 9 as a magic-number isn't as well known* but there is some precedent for using the term "magic-number" when referring to to the number 9. For example, "casting out nines" and a related one called calculating the "digital root" of a number, also involving the number 9.

So the musical-math-lesson is legit, assuming that Jack is referring to this fact about 9:

The sum-of-the-digits-of-a-number is divisible by 9,
if and only if,
the number is divisible by 9.

For example:

$$9^5 = 9 \cdot 9 \cdot 9 \cdot 9 \cdot 9 = 59049 \quad \text{and} \quad 5 + 9 + 0 + 4 + 9 = 27 \quad \text{where} \quad \frac{27}{9} = 3.$$

But 3 is also has this magic-number property, for example:

$$3 \cdot 67 = 201 \quad \text{and} \quad 2 + 0 + 1 = 3$$

In this case, 9 does not divide 201† but 3 does (67 times). We can see that adding up the digits of 201 gives us 3, which of course is divisible by 3, but not by 9.

So given that the term "magic-number" hasn't got a formal definition in the math world, I think it's time to give it one. How about if we call ANY number that has this divisibility property (with respect to adding up the digits of another number) a "magic-number"?

Too bad 3 and 9 are the only magic-numbers in base-10, but what about other bases? The Heptapods in the film "Arrival" have 7 limbs, 3 arms and 4 legs, with 7 fingers/toes each. I'm guessing that they probably use some form of positional-notation, but instead of base-ten they probably use base-7, base-21, or base-49‡, so they might have different magic-numbers from us.

Let's examine some numbers converted from our familiar base-ten to different bases. In each example, let's multiply the base-minus-1 with some other number. 268 is our first example,

*According to my own *highly scientific (cough cough)* informal poll conducted on Facebook, "9" is NOT the first thing that pops into people's heads when they hear the phrase "magic-number" - in fact no one answered "9" in my poll.

†Why is it immediately apparent that 9 does not divide 201? Hint: both 3 and 67 are prime numbers. Check the "Fundamental Theorem of Arithmetic" wiki page for further insight.

‡For an understanding of alternate bases please see the paper "Counting"

which is 4 times 67 but we'll look at it in base-5. Notice how the sum of the digits of the base-5 representation of 268 is divisible by 4.

$$\begin{array}{lllrl}
4 \cdot 67 = 268 & \text{in base-5 is } (2033)_5 & \text{but} & 2+0+3+3=8 & \text{and } (\frac{8}{4}=2) \\
7 \cdot 181 = 1267 & \text{in base-8 is } (2363)_8 & \text{but} & 2+3+6+3=14 & \text{and } (\frac{14}{7}=2) \\
15 \cdot 23 = 345 & \text{in base-16 is } (159)_{16} & \text{but} & 1+5+9=15 & \text{and } (\frac{15}{15}=1) \\
20 \cdot 908249 = 18164980 & \text{in base-21 is } (498991)_{21} & \text{but} & 4+9+8+9+9+1=40 & \text{and } (\frac{40}{20}=2) \\
30 \cdot 35951 = 1078530 & \text{in base-31 is } (15699)_{31} & \text{but} & 1+5+6+9+9=30 & \text{and } (\frac{30}{30}=1)
\end{array}$$

Notice the pattern in our examples: $b-1$ acts like a magic-number in base-b. In the first example 4 divides 268 (sixty-seven times), but when writing out 268 in base-5 we can see that the sum of those digits is also divisible by 4.

Similarly in the second example 7 divides 1267, and 1267 written in base-8 shows us that the sum of those digits is also divisible by 7. Similar story with the remaining examples.

Let's take a look at some other examples in base-31. It appears that 2, 3, 5, 6, 10, 15 (along with 30 above) might *all* be magic-numbers in base-31:

$$\begin{array}{rllrr}
2 \cdot 409 \cdot 1129 & = 923522 & = (10001)_{31} & \text{and} & 1+0+0+0+1=2 \\
3 \cdot 641 & = 1923 & = (201)_{31} & \text{and} & 2+0+1=3 \\
5 \cdot 139 \cdot 2659 & = 1848005 & = (20102)_{31} & \text{and} & 2+0+1+0+2=5 \\
6 \cdot 10091 & = 60546 & = (2103)_{31} & \text{and} & 2+1+0+3=6 \\
10 \cdot 197 \cdot 941 & = 1853770 & = (20701)_{31} & \text{and} & 2+0+7+0+1=10 \\
15 \cdot 71503 & = 1072545 & = (15027)_{31} & \text{and} & 1+5+0+2+7=15
\end{array}$$

See the pattern? All the divisors of 30 seem to be magic-numbers in base-31. It turns out that in base-b, then any divisor of $(b-1)$ is a magic-number in base-b; however, since we've only looked at some examples, we can't make that claim unless we prove it in general.

What about 1? Wouldn't 1 a magic-number in all bases? Of course it would because we know that all numbers are divisible by 1, and adding up any set of digits is also divisible by 1, but this isn't very interesting so let's exclude 1 from being considered as a magic-number - it's not helpful information.

Let's review what it means for a number to be divisible by another number*.

Euclidean Division Theorem

For all integers a and b such that $b \neq 0$, there exist *unique* integers q and r such that:

$$a = qb + r; \text{ where } 0 \leq r < |b|$$

Definition: In the above equation†:

a is the *dividend*	("the number being divided")
b is the *divisor*	("the number doing the dividing")
q is the *quotient*	("from Latin *quotiens* 'how many times' b goes into a")
r is the *remainder*	("what's left over (if anything) after the division")

Which is how you learned to divide in primary school with "long-division", that is;

$$\frac{a}{b} = q, \text{ with remainder } r$$

So for example.

$$\frac{19}{6} = 3, \text{ with remainder } 1$$

So to say that a is divisible by b simply means‡ that r is zero so we can write:

$$a = q \cdot b \qquad \text{or} \qquad \frac{a}{b} = q$$

We express the fact that a is divisible by b, and say "b divides a" using this notation:

$$b \mid a$$

So the following is always true:

$$1 \mid a, \text{ and } a \mid a;$$

also

$$b \mid 0 \text{ for every } b \text{ except } 0$$

In order to create our theorem with a nice definition for "magic-number" we need to remind ourselves what it means to write a number in a given base§:

Basis Representation Theorem

Let b be a positive integer greater than 1.

For every positive integer n there is a unique sequence of integers $d_0, d_1, d_2, \ldots, d_k$ such that:

$$n = d_k b^k + d_{k-1} b^{k-1} + \cdots + d_2 b^2 + d_1 b^1 + d_0 b^0,$$

where $0 \leq d_i < b$ for all i in $\{0, 1, 2, \ldots, k\}$ and $d_k \neq 0$.

Definition: n is represented in base-b by the string of base-b-digits $(d_k d_{k-1} \cdots d_2 d_1 d_0)_b$

*"Counting" p. 21

†Recall that $|b|$ means the "absolute value" of b and is always positive. For example $|-13| = 13$.

‡Paraphrased from "An Introduction to the Theory of Numbers" by G. H. Hardy and E. M. Wright. Pg 1.

§"Counting p. 2"

Armed with our divisibility notation above plus what it means to express an arbitrary number in a given base we can state our new theorem as follows.

Magic-Number Theorem

> Let $n = d_k b^k + \cdots + d_2 b^2 + d_1 b^1 + d_0 b^0$ be the base-b-representation of n.
>
> If m is a positive integer such that $m \mid (b-1)$ then*,
>
> $$m \mid n \qquad \Leftrightarrow \qquad m \mid (d_k + \cdots + d_2 + d_1 + d_0)$$
>
> Definition: $m \neq 1$ is called a "magic-number in base-b".

As an interesting side note - according to our definition, binary, or base-2, doesn't have a magic-number. No great loss, as we said above 1 isn't helpful to consider as a magic-number.

Let's prove the magic-number-theorem using modular-arithmetic. If you aren't familiar with modular-arithmetic then check out Khan Academy's "What is modular-arithmetic?". Khan's introductory explanation is excellent, simple and clear, as is the entire Khan Academy site in case you've never checked it out.

If we take the a, b, q and r from the Euclidean Division Theorem above where:

$$a = qb + r \text{ such that } 0 \leq r < |b|$$

Then the "mod" operator is defined like this:

$$a \bmod b = r$$

To prove our theorem we need to prove that the remainder of n divided by m is zero, if and only if, the remainder of $d_k + \cdots + d_1 + d_0$ divided by m is also zero. Restated in terms of modular-arithmetic, we need to prove:

$$n \bmod m = 0 \qquad \Leftrightarrow \qquad (d_k + \cdots + d_1 + d_0) \bmod m = 0$$

I'm going to assume that you are familiar with how to use modular-arithmetic from this point forward; if not, make a quick detour to Khan Academy.

Lemma

Let $b > 1$ and m be positive integers such that $m \mid (b-1)$ then,

$$b^k \equiv 1 \pmod{m}, \text{ for all integers } k \geq 0$$

*Recall that the bidirectional arrow symbol $\Leftrightarrow$ means "if and only if" - it's like a logical "equals" sign, the truth of one implies the truth of the other.

Proof of Lemma

Let k, b and m be integers as described in the lemma, then there exists an integer q such that,

$$\begin{aligned} & m \cdot q = b - 1 && \text{(Definition of } m \mid (b-1)\text{)} \\ \Leftrightarrow \quad & m \cdot q + 1 = b && \text{(Add 1 to both sides)} \end{aligned}$$

Given this equality we can state the following modular-congruence:

$$\begin{aligned} & m \cdot q + 1 \equiv b && \pmod{m} \\ \Leftrightarrow \quad & 0 \cdot q + 1 \equiv b && \pmod{m} \quad \text{(Since } m \bmod m = 0\text{)} \\ \Leftrightarrow \quad & 1 \equiv b && \pmod{m} \end{aligned}$$

Furthermore,

$$\begin{aligned} & 1 \equiv 1^k && \pmod{m} \quad \text{(For all } k >= 0\text{)} \\ \Leftrightarrow \quad & 1 \equiv b^k && \pmod{m} \quad \text{(Substitute } b \text{ for 1 since they are congruent)} \end{aligned}$$

QED

Proof of Magic-Number Theorem

Let b be a positive integer greater than 1.

Let $n = d_k b^k + \cdots + d_2 b^2 + d_1 b^1 + d_0 b^0$ be the base-b-representation of n. Also let m be a positive integer such that $m \mid (b-1)$. Therefore,

$$\begin{aligned} & n = d_k b^k + d_{k-1} b^{k-1} + \cdots + d_2 b^2 + d_1 b^1 + d_0 b^0 \\ \Rightarrow \quad & n \equiv d_k b^k + d_{k-1} b^{k-1} + \cdots + d_2 b^2 + d_1 b^1 + d_0 b^0 && \pmod{m} \\ \Leftrightarrow \quad & n \equiv d_k \cdot 1 + d_{k-1} \cdot 1 + \cdots + d_2 \cdot 1 + d_1 \cdot 1 + d_0 \cdot 1 && \pmod{m} \quad \text{(By lemma)} \\ \Leftrightarrow \quad & n \equiv d_k + d_{k-1} + \cdots + d_2 + d_1 + d_0 && \pmod{m} \end{aligned}$$

Therefore n is congruent to the sum of its digits mod m, furthermore $m \mid n$ if and only if:

$$\begin{aligned} & 0 \equiv n && \pmod{m} \quad \text{(Definition of } m \mid n\text{)} \\ \Leftrightarrow \quad & 0 \equiv d_k + d_{k-1} + \cdots + d_2 + d_1 + d_0 && \pmod{m} \quad \text{(Substitute sum of digits for } n\text{)} \end{aligned}$$

QED

Epilogue

It’s amazing how simple is is to prove our theorem using modular arithmetic. I believe the magic-number-theorem isn’t usually granted any special status (like giving it a name and adding a new definition for “magic-number”) and is likely only presented as a simple exercise for students in elementary-algebra or elementary-number-theory textbooks.

However, it’s fun and I want to use this theorem and some other observations about times-tables to see if I can determine what the “best” base-number-system might be! (I’ll define “best” later.) At any rate, I think the Heptapods in “Arrival” might be the winners with base-21. Stay tuned for that paper!